

# **Security Guidelines for Intensity Frontier (IF) Experiments Offline Production [ID 5644]**

The Intensity Frontier (IF) experiments at Fermilab have large-scale production and analysis workflows, which include tasks like the execution of automated job submissions with autonomous data handling. IF experiments are big scientific collaborations using the grid resources actively to extract meaningful output from the collected data. Most of these experiments use service certificates and shared accounts to achieve the collaborative environment where the tasks and the output data need to be accessible and manageable by a big group of people from different institutions located around the globe.

The Scientific Computing Information Security group (SCIS) has prepared this document, which provides guidelines to the experiments for service certificate management and the appropriate use of shared accounts in compliance with the Fermilab Security Policy.

## **ABOUT THE SERVICE CERTIFICATE MANAGEMENT**

In order to setup automated job submission for offline production and additional scientific data processing tasks, IF experiments use Open Science Grid (OSG) service certificates. The service certificates are useful for daily continuous production, because the proxy generation does not prompt for the passphrase to unencrypt the private key; the proxy can be automatically generated without human intervention. The service certificates are requested through the OSG Information Management (OIM) interface by someone representing the experiment and who will take the responsibility as certificate owner. Additionally, handling service certificates is a sensitive task: the private key – provided separately at certificate issuance- is not encrypted and any person can use it to impersonate the service.

According to Fermilab Security Policy, certificate owners obligations include:

*"Exercise all reasonable care in protecting the private keys corresponding to their certificates, including but not limited to never storing them on a networked file system or otherwise transmitting them over a network."*

As an alternative, it is strongly recommended that IF experiments delegate their service certificate management to User Support for Distributed Computing group (USDC). USDC will request the service certificate on behalf of the experiment and after certificate

issuance, will manage the certificate and private key according to the Fermilab Security Policy. USDC responsibilities regarding the management of service certificates belonging to Intensity Frontier experiments are:

- Request the OSG service certificate on behalf of the IF experiment. The experiment is required to provide contact person information for this request.
- Store the service certificate and the private key in a secure machine with limited access.
- Generate the X.509 VOMS proxy derived from the service certificate and store it in a designated area accessible from experiment interactive nodes (submission nodes).
- Guarantee the existence of a valid VOMS proxy in the designated area by generating a new proxy instance before the current one expires.

## ABOUT THE SHARED ACCOUNTS

IF experiments use shared accounts, known as “*production*” accounts to share a common working area, schedule jobs for production and enable scientific collaboration. The access to this shared account is controlled through the file *.k5login*. As the MIT Kerberos documentation states, the *.k5login* file, which resides in a user’s home directory, contains a list of the Kerberos principals. Anyone with valid tickets for a principal in the file is allowed host access with the UID of the user in whose home directory the file resides.

These are the established rules by SCIS for the use of shared accounts:

- Maximum 10 kerberos individual principals are allowed in the *.k5login* file. This maximum number does not include OPOS operators and SCD support.
- Only service principals managed directly by SCD personnel are allowed in the *.k5login*.
- All SSH sessions will be terminated after 60 minutes of inactivity. This control will be implemented in the interactive nodes **[experiment]gpvm[01-10]**.
- Given the importance of the “*production*” account, there is no maximum of simultaneous SSH connections in the shared accounts.

## References:

- [https://security.fnal.gov/policies/pki\\_policy\\_certification\\_practices.htm](https://security.fnal.gov/policies/pki_policy_certification_practices.htm)
- <https://twiki.grid.iu.edu/bin/view/Documentation/SecurityUserResponsibilities>
- [https://twiki.opensciencegrid.org/twiki/bin/viewfile/VirtualOrganizations/WebHome/OSG\\_VO\\_AUP.pdf](https://twiki.opensciencegrid.org/twiki/bin/viewfile/VirtualOrganizations/WebHome/OSG_VO_AUP.pdf)
- [http://web.mit.edu/kerberos/krb5-1.13/doc/user/user\\_config/k5login.html](http://web.mit.edu/kerberos/krb5-1.13/doc/user/user_config/k5login.html)